

ABSTRACT

The invention relates to a data protection method using a cryptographic algorithm comprising at least one execution cycle of repetitive operations for processing data elements (K2, R1) so as to generate encrypted information (C) this method comprising at least one step (120, 220) for randomly modifying the execution of at least one operation from one cycle to another, or at least one of the data elements, so that the encrypted information is unchanged by this random modification.